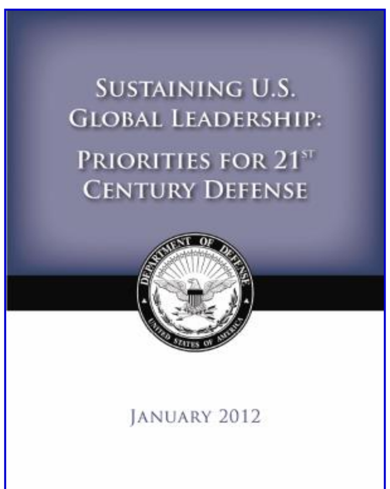
Maintaining Our Technological Advantage in an Era of Uncertainty: *Scarce Resources, Agility & Innovation*

Al Shaffer
Acting Assistant Secretary of Defense for Research and Engineering

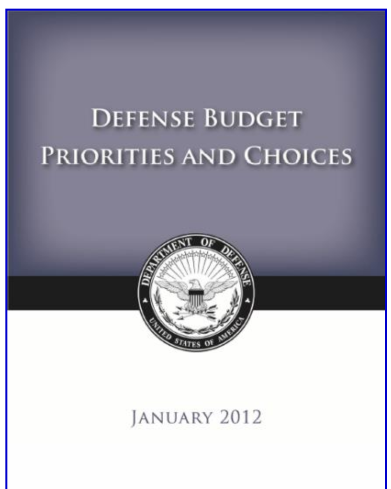
01 April 2014

Key Elements of Defense Strategic Guidance


SUSTAINING U.S. GLOBAL LEADERSHIP:

PRIORITIES FOR 21ST CENTURY DEFENSE

JANUARY 2012


DEFENSE BUDGET PRIORITIES AND CHOICES

JANUARY 2012

- The military will be smaller and leaner, but it will be agile, flexible, ready and technologically advanced.
- Rebalance our global posture and presence to emphasize Asia-Pacific regions.
- Build innovative partnerships and strengthen key alliances and partnerships elsewhere in the world.
- Ensure that we can quickly confront and defeat aggression from any adversary – anytime, anywhere.
- Protect and prioritize key investments in technology and new capabilities, as well as our capacity to grow, adapt and mobilize as needed.

DoD at Strategic Crossroads

Chuck Hagel
Budget Roll Brief
24 Feb 2014

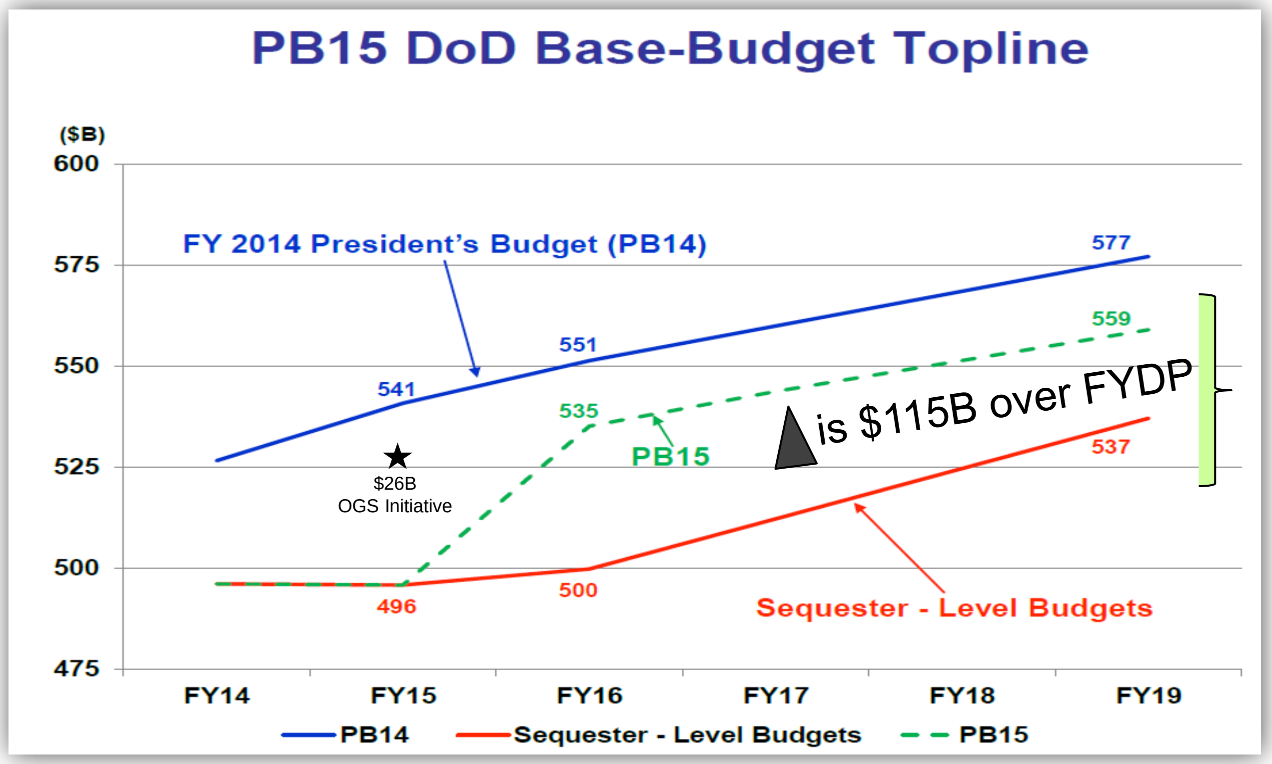
"The development and proliferation of more advanced military technologies by other nations means that we are entering an era where American dominance on the seas, in the skies, and in space can no longer be taken for granted"

The strategic question is – will the force of tomorrow be:

- Larger with diminished capability or,
- Smaller with more technologically advanced capabilities

Strategic Future and Fiscal Uncertainty

"In the next 10 years, I expect the risk of interstate conflict in East Asia to rise, the vulnerability of our platforms and bases to increase, our technology edge to erode, instability to persist in the Middle East, and threats pose by violent extremist organizations to endure. Nearly any future conflict will occur on a much faster pace and on a more technically challenging battlefield."

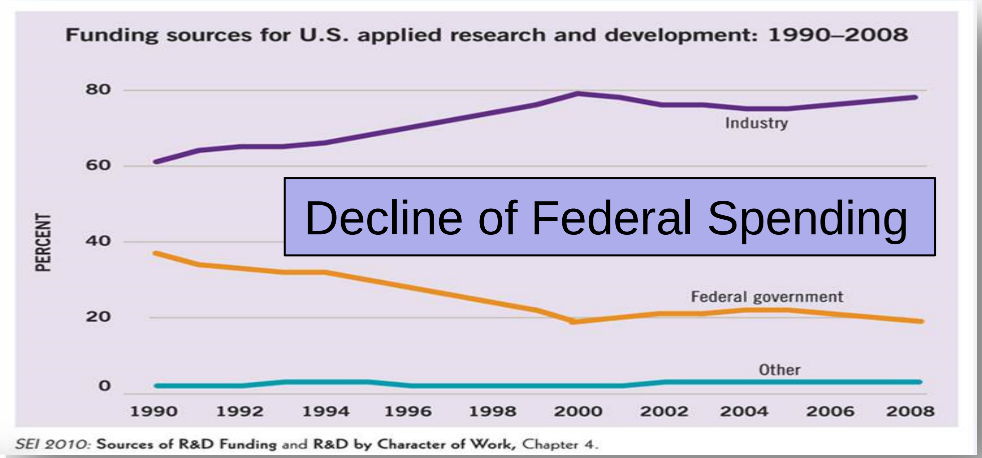


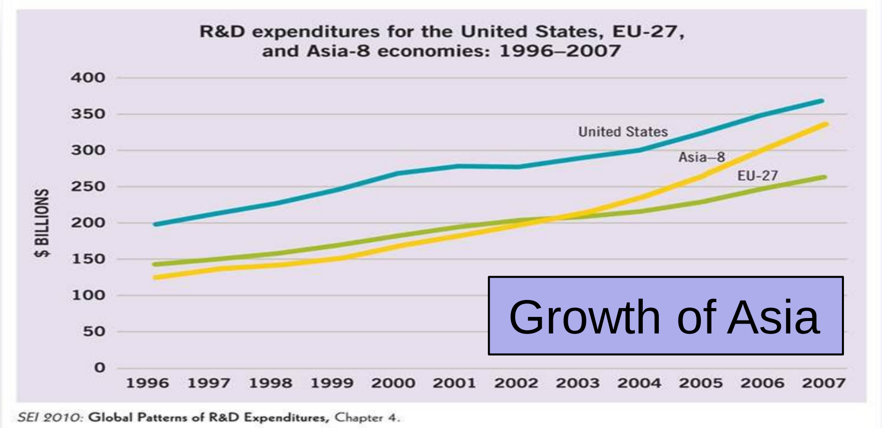
OGS: Opportunity, Growth, and Security

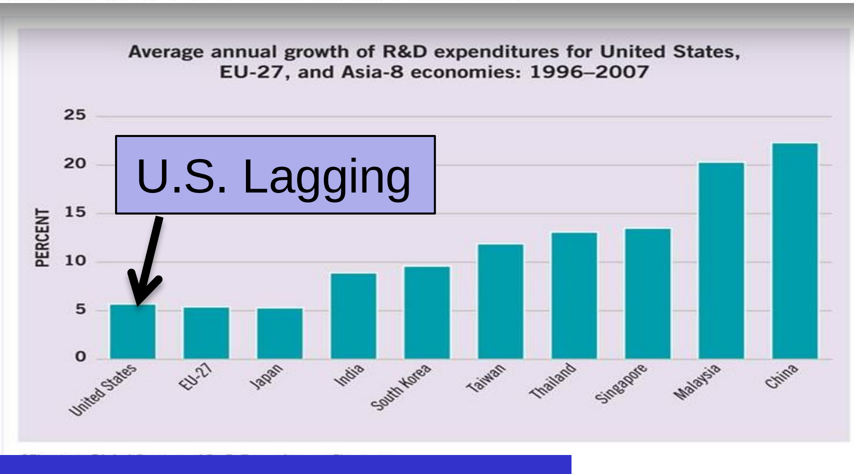
GEN Dempsey, CJCS
QDR Assessment

Globalization of Technology

Global technology development is changing rapidly

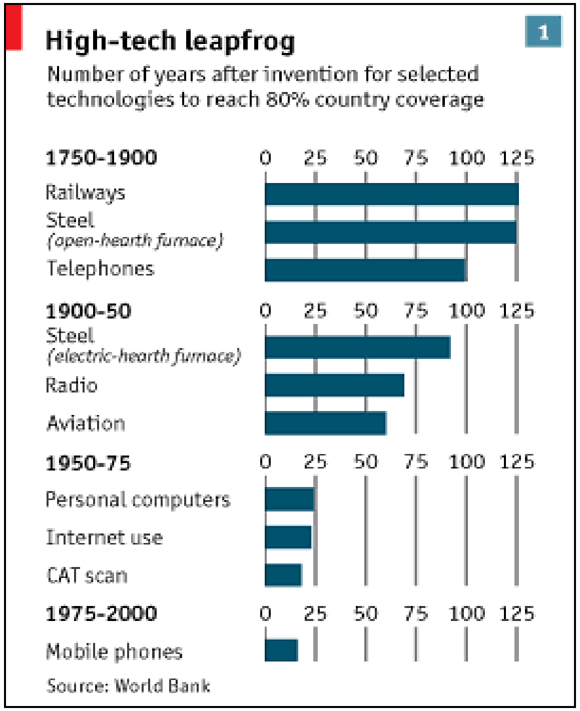




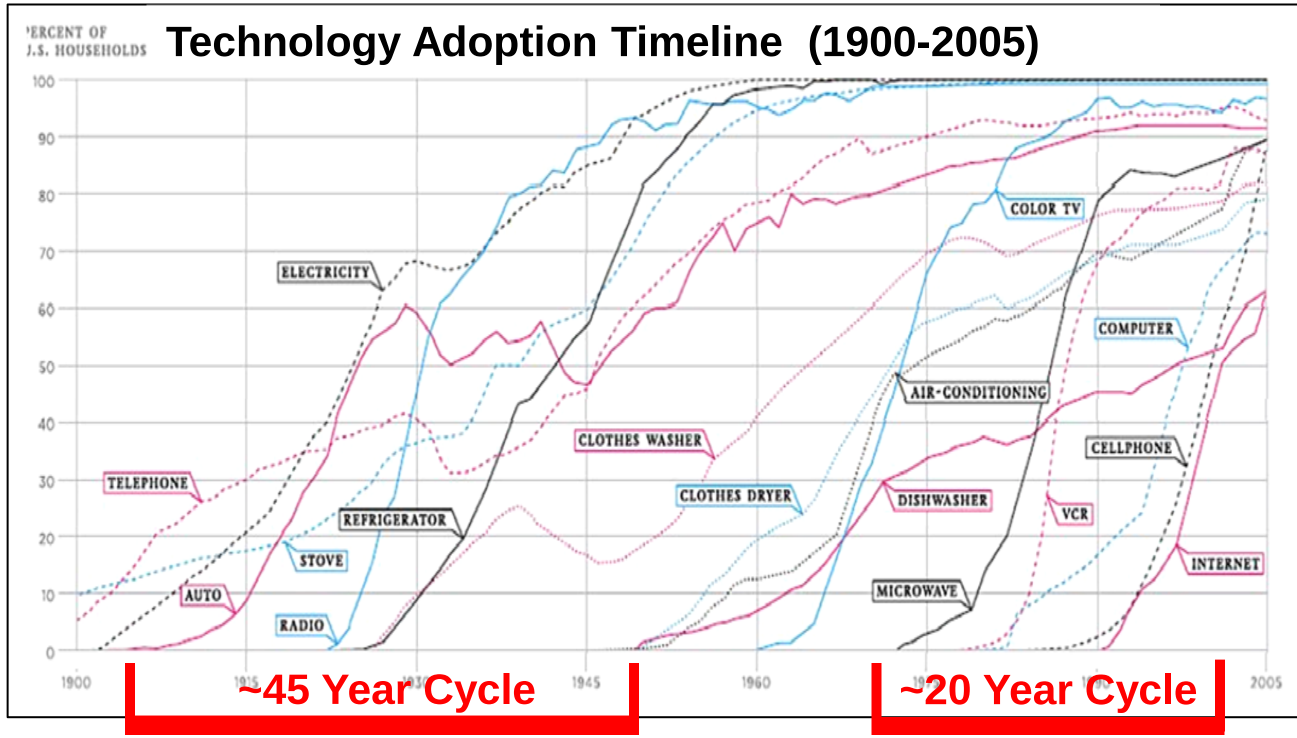


These changes *will* affect our future

Pace of Technology



The Economist, Feb. 9, 2008



It took 23 years to go from modeling germanium semiconductor properties to a commercial product

The carbon nanotube was discovered in 1991; recognized as an excellent source of field-emitting electrons in 1995, and commercialized in 2000

The Pace of Technology Development and Market Availability is Exceeding the Pace of Acquisition

Defense R&E Strategy

"Protect and prioritize key investments in technology and new capabilities, as well as our capacity to grow, adapt and mobilize as needed."

-SECDEF, January 2012 Strategic Guidance

1. Mitigate new and emerging threat capabilities

- Cyber
- Counter Space
- Electronic Warfare
- Counter-WMD

2. Affordably enable new or extended capabilities in existing military systems

- Systems Engineering
- Prototyping
- Interoperability
- Modeling and Simulation
- Developmental Test & Evaluation
- Power & Energy

3. Develop technology surprise through science and engineering

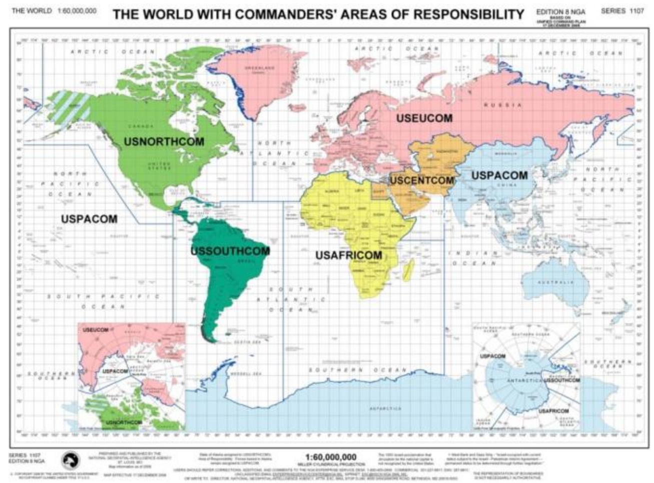
- Autonomy
- Human Systems
- Quantum
- Data-to-Decisions
- Hypersonic

Technology Needs

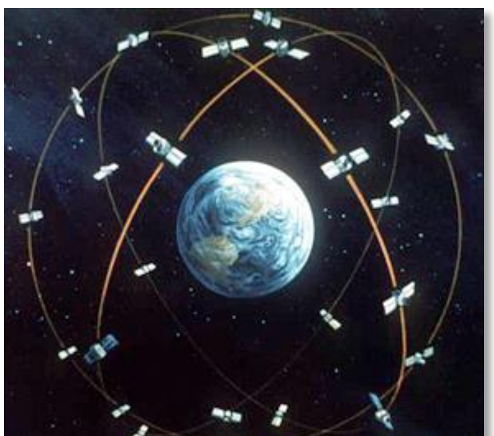
- Cyber / Electronic Warfare
- Engineering / M & S
- Capability Prototyping
- Protection & Sustainment
- Advanced Machine Intelligence
- Anti-Access/Area Denial (A2/AD)

Rise of the Commons

Electronic Warfare

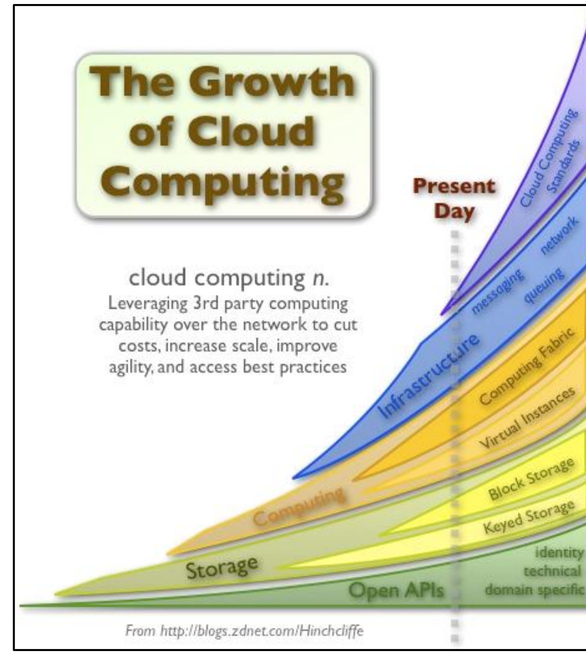


Oceans



Space

Cyber



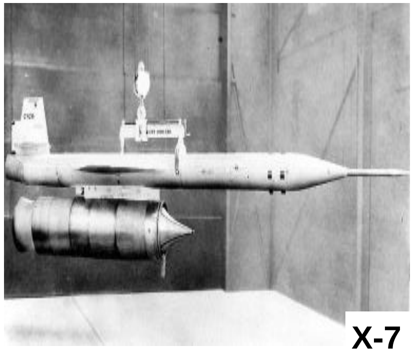
Ubiquitous Data

Military Operations Increasingly Depend on Being Able to Operate in Places "No One Owns" – *The Enablers*

Capability Prototyping
Proof of Concept: “X”- Plane Prototyping

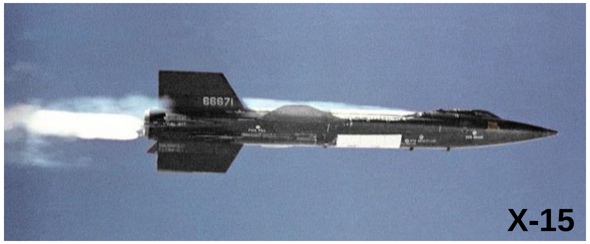
First flight: 1947
Speed: Mach 1.26

First flight: 1952
Speed: Mach 3.2



First Flight: 1951
Speed: Mach 4.31

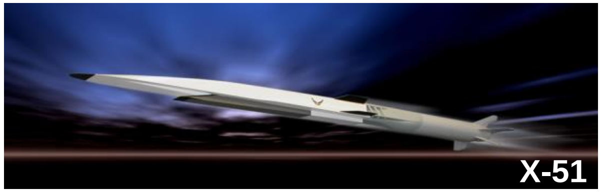
First Flight: 1953
Speed: Mach 2



First Flight: 1959
Speed: Mach 6.7

X-43

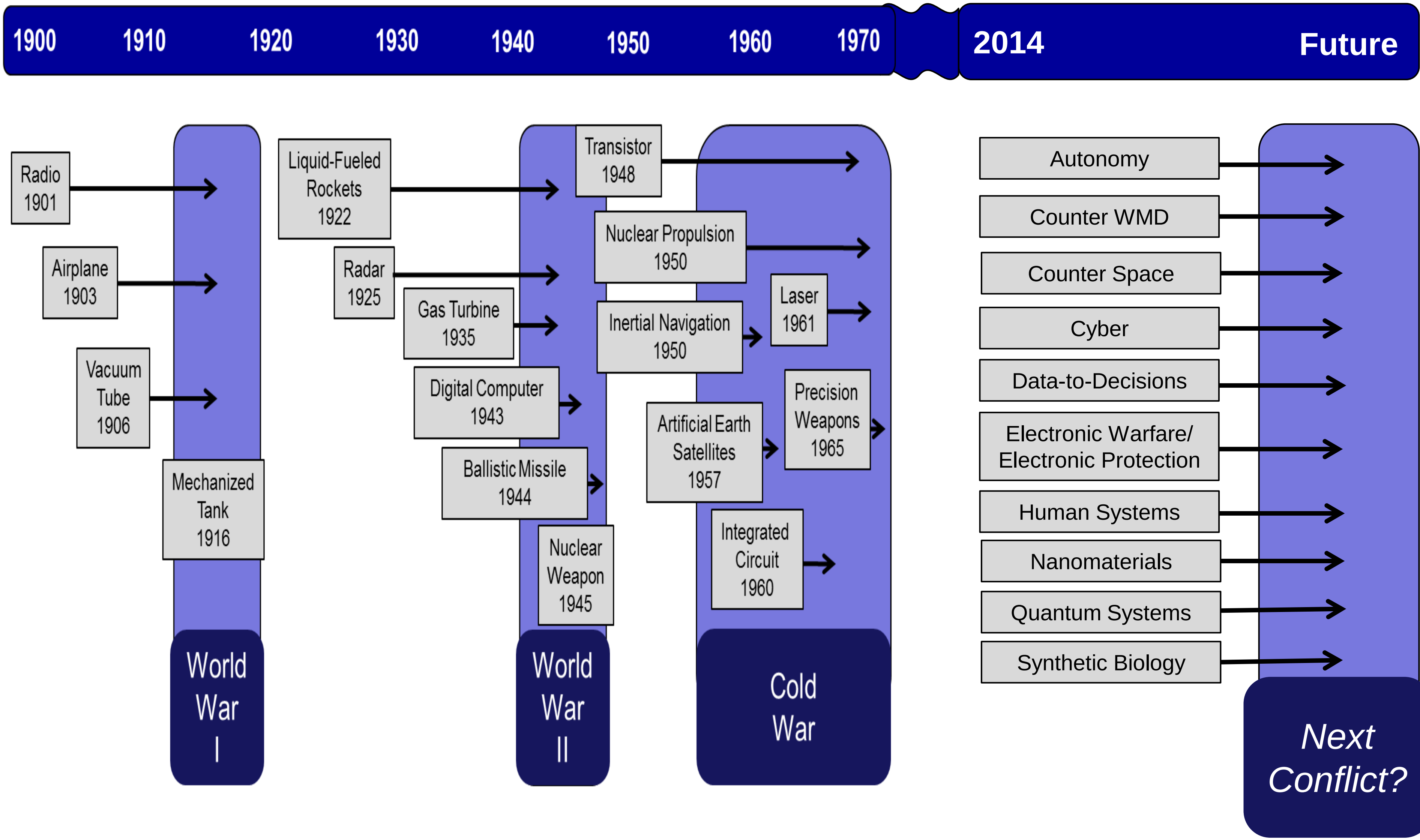
First Flight: 2001
Speed: Mach 6.83



First Flight: 2010
Speed: Mach 5.1

The Department can cost-effectively drive innovation in aviation, space, maritime and ground combat systems through prototyping

Lab Demo to Forcing Function: Technology Investment Stocks Cupboard



The Microelectronic Field moves *faster* than Acquisition

1.25um CMOS
1.0 / 0.8 / 0.5 um CMOS
0.35 um CMOS
0.25 um CMOS
0.18 um CMOS
130 nm CMOS
90 nm CMOS
65 nm CMOS

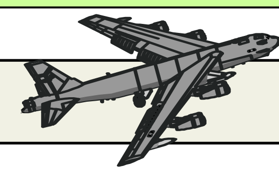
Mil Apps predominately:
-SOTP & Low Volume
- Example: NG's systems use 96% >= 0.25 um (2009 statistics)

Legend:
VHSIC-Very High Speed Integrated Circuit
SOS/SOI-Silicon on Sapphire/Insulator
SiGe-Silicon Germanium
SOTP-State of the Product
CMOS-Complementary metal oxide semiconductor
Cu-Copper
K-Potassium

VHSIC
Early work on SOS/SOI
Planar Multi-level Metal
SiGe
SOI
Cu and Low K
High-K Gate Insulator

1980 1990 2000 2010

1946 1955 **B-52** 2040+ **94+ Years**

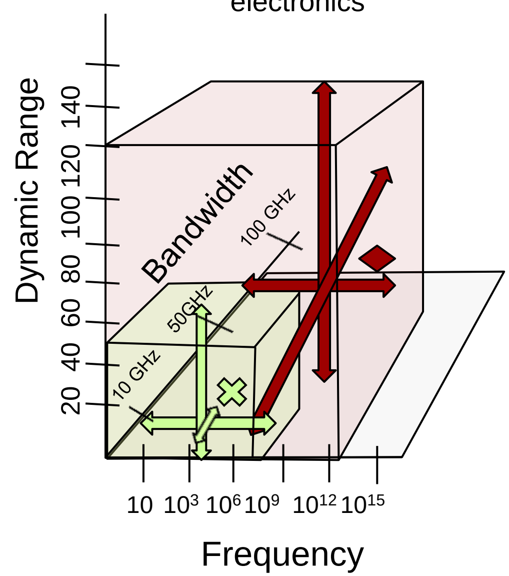


Distribution Statement A: Approved for public release; distribution is unlimited

Electronic Warfare Battlespace

ACE- [Advanced Components for Electronic Warfare (ACE) Research]
Conventional electronics

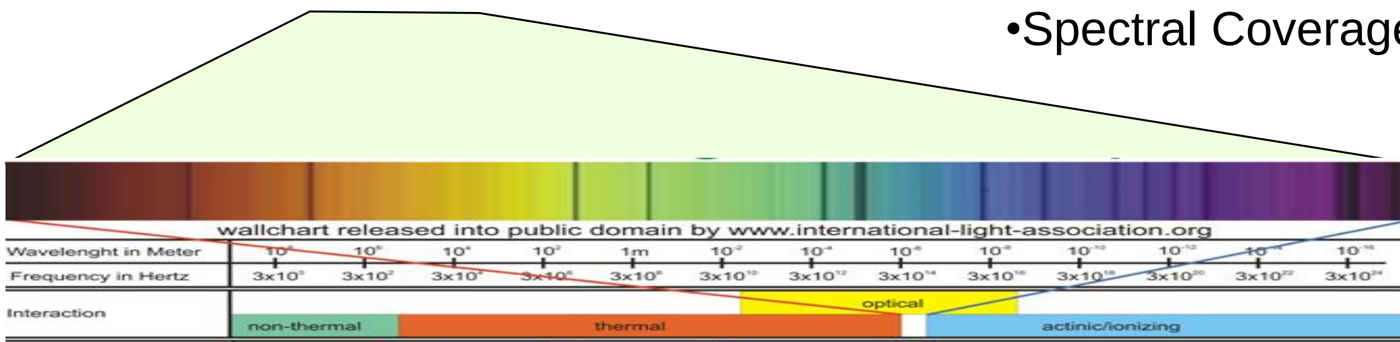
- Linearity (L)
- Bandwidth (BW)
- Frequency (f)
- Agility (a)
- Pulse Duration (PD)
- Signal-to-Noise Ratio (SNR)



- Detection Range

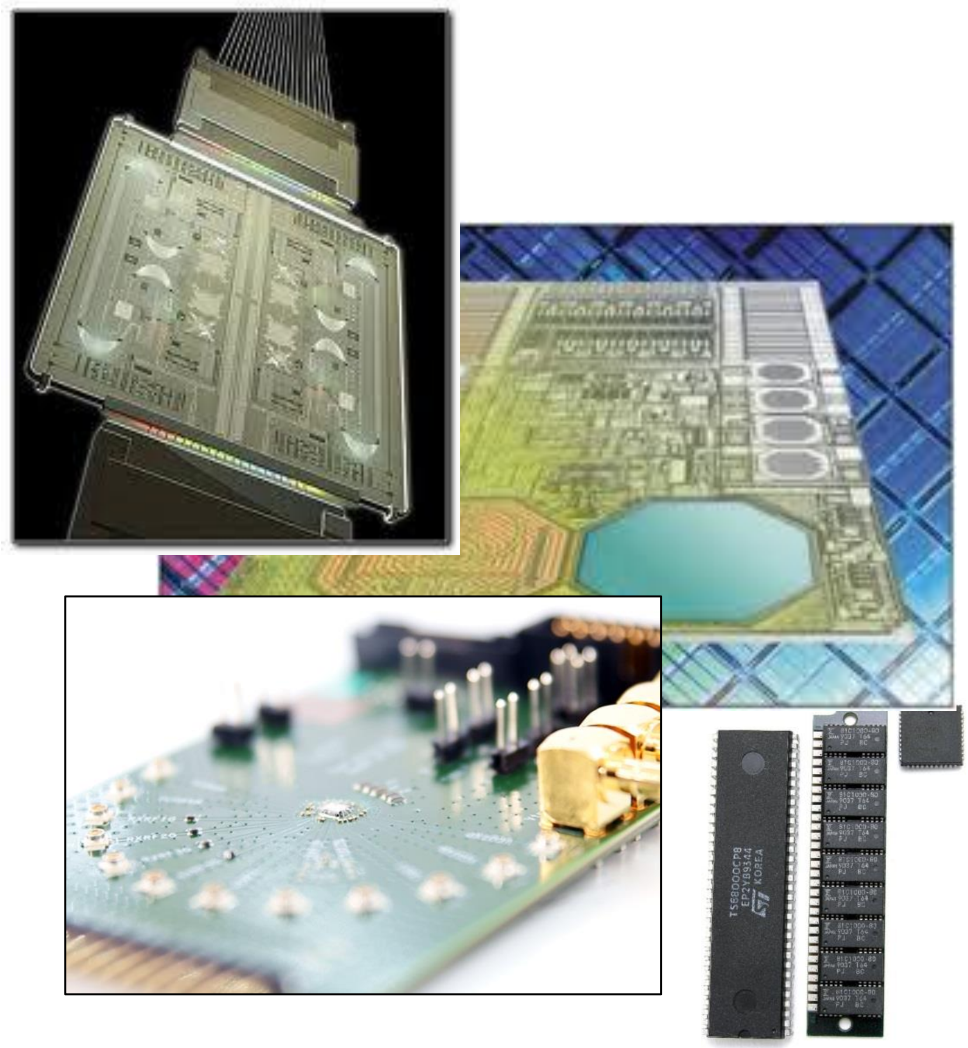
  f (L, BW, SNR)

  - Target Identification
  - Countermeasure Rejection
- High-density
  - High Speed
  - Spectral Coverage



ACE
Four Interdependent Thrusts

- **Thrust 1 -** Integrated Photonics Circuits (IPC)
- **Thrust 2 -** Millimeter Waves Sources, Receivers and Components (MMW)
- **Thrust 3 -** Reconfigurable and Adaptive RF Electronics (RARE)
- **Thrust 4 -** 3 Dimensional Heterogeneous Integrated Photonic Circuits (3D-HIPS)



Vital Infrared Sensor Technology Acceleration (VISTA) Program

- High-performance infrared (IR) Focal Plane Arrays (FPA) are key components of all US and foreign military and commercial IR sensor systems
- Chartered Technology Focus Team in November 2008 concluded:
  - US historic advantage in IR sensors is eroding
  - Improving adversarial capability and asymmetric RoE put friendly forces at higher risk
  - New technical opportunities allow leap-ahead capabilities
  - Prevailing DoD technology - mercury cadmium telluride (MCT or HgCdTe) - has serious drawbacks
- Responded with multi-pronged Joint effort through PBR 11-15 issue cycle

November 2008 Assessment

Capabilities	UK	France	Germany	Israel
High Perf LWIR	=	=	=	
Low Cost	MCT/GaAs (Selex)	QWIPs (Thales)	=	
High Perf MWIR	=	=	=	=
Low Cost	MCT/GaAs (Selex)	=	=	
Large Format MWIR or LWIR				
Dual Band (MWIR/LWIR)	=	=		
Low Cost	MCT/GaAs (Selex)	=	=	
Dual Color MWIR			SLS (AIM)	
Very Longwave IR				
Active SWIR	MCT (Selex)	=		
TE Cooled (HOT) MW	=			=
Uncooled IR		=		=

U.S. superior to Foreign

U.S. equivalent to Foreign

U.S. behind Foreign

No foreign investment, very little US investment

7 years ago was all green - U.S. is losing the lead in IR sensor technology

Without addressing this issue, U.S. forces will lose control of the night

VISTA Summary

VISTA program is arresting erosion of U.S. asymmetric warfighting advantage in IR sensors

- Significant technical breakthroughs advancing performance and enabling new operational capabilities
- VISTA products targeted on acquisition insertion opportunities across the warfighting domains
- VISTA program is making rapid progress in new III-V IR Focal Plane Arrays (FPA) technologies
  - Moving industrial capabilities to the next level of performance
- Continue to monitor foreign progress to maintain leap ahead capabilities

Technology Superiority built on the backbone of *Defense Microelectronics*

- Defense Microelectronics
  - Nanoelectronics & Microelectronics
    - Budget Activities 1-3 *(Basic Research, Applied Research, Advanced Technology Development)*
  - Microelectronics Challenges
  - Reliability Timeline
  - Future Technologies Direction

Defense Microelectronics

- **DoD heavily relies on microelectronics – Understanding, assessments and advancements are needed**
  - Beyond traditional Moore's Law
  - Significant reductions in size, weight, power and cost
  - Higher levels of reconfigurability and tunability
  - Thermal management and use in harsh environments
  - Trustworthiness – supply chain cost and risk, lifetime and tamper-proof

- **DoD's Advanced Electronics Community of Interest ensures a highly integrated strategy and execution – Army, Navy, AF, DARPA, DMEA**
  - **Basic Research** – **Nanoelectronics** - materials-to-devices
  - **Applied Research** – **Nanoelectronics** - devices-to-circuits
  - **Advanced Technology Development** – **Microelectronics** - reduce microelectronics supply chain risk

- **Commercial applications drive the leading edge in microelectronics, but DoD still strongly influences industry through savvy and targeted R&D investments producing technology breakthroughs**

High Level Nanoelectronics S&T Strategy
(Basic Research)

- Partnerships with industry and academia
  - III-IV’s Integrated with Silicon Nano-Wire Complementary metal oxide semiconductor (Si CMOS)
  - Carbon Based
  - Reduced Power Dissipation
- DARPA STARNet- challenging problems to advancing microsystems beyond Moore’s Law
- Phenomenology for Trust- Field Programmable Gate Array (FPGA) vendors gain better insight into supply chains
- Degradation stressors and mechanisms- HiREV programs developing a physics based approach to replace statistics-driven projections
  - Characterizing atomistic and interfacial phenomena
  - Developing and applying multi-scale materials models to model and simulate degradation rates

High Level Nanoelectronics S&T Strategy
(Basic Research cont.)

- Quantum information science including:
  - Information Processing
  - Computing
  - Reduced Power Dissipation
  - Sensing
  - Key Distribution

- New Architectures/Algorithms Toward Cognition including:
  - Digital Clock Rates Exceeding 15 GHz
  - Integration of Integrated Photonic Circuits & Electronic Integrated Circuits (IC's) From Extraordinary Powerful Energy Efficient Processors
  - Biomimetic Inspired Electronics

High Level Nanoelectronics S&T Strategy
(Applied Research)

- Provides analysis and assessment of current technology capability readiness to acquisition community
  - Better understand costs, risks and benefits of various supply chains

- Microelectronics Supply Chain- Studying the feasibility of a trusted supply chain

- ROI for Trustworthiness- assess the Return on Investment (ROI) for Trust
  - DMEA developing quantitative techniques for risk indexing and working with industry to develop high volume, low-cost, timely trustworthiness assessment tools using:
    - Reverse engineering
    - High performance computing techniques

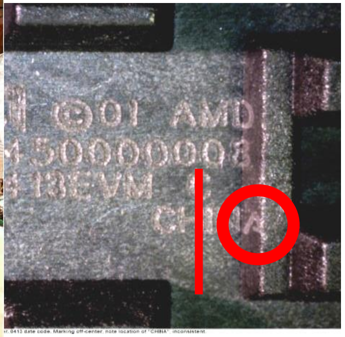
- Highly integrated microsystems including:
  - Leveraging Trusted Foundry advanced Silicon Germanium & Silicon Complementary metal oxide semiconductor technologies producing Radio Frequency and mixed-signal Integrated Circuits & SOCs targeted for Electronic Warfare, Radar and Communication

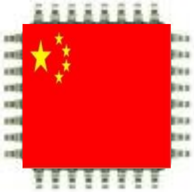
High Level Microelectronics S&T Strategy
(Advanced Technology Development)

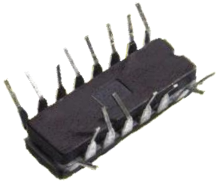
- S&T to reduce microelectronics supply chain risk
- DARPA SHIELD and other anti-counterfeiting techniques
- Methods to provide relatively high speed non-destructive inspection of entire devices to detect malicious inclusions
- DMEA provides microelectronic engineering solutions utilizing more advanced technology and is the source of last resort for legacy microelectronics – those both obsolete and unavailable due to DoD’s low volume, high mix requirements
- Demonstrate capability through targeted demonstrations of advanced microelectronics
- FY14: 90nm Silicon Germanium Bi-Complementary metal oxide semiconductor (Bi-CMOS) and 14nm CMOS Multi-Project Wafer runs at the leading edge Trusted Foundry (IBM)

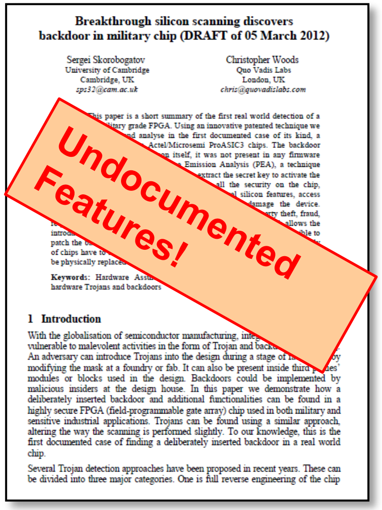
Microelectronics Challenges for Defense Systems

- Assurance / Availability / **Reliability**
- Growing counterfeit industry
- Managing **Complexity**
- **Globalization** of leading components









Breakthrough silicon scanning discovers backdoor in military chip (DRAFT of 05 March 2012)

Sergei Skorobogatov
University of Cambridge
Cambridge, UK
sps32@cam.ac.uk

Christopher Woods
Quo Vadis Labs
London, UK
chris@quovadislabs.com

This paper is a short summary of the first real world detection of a [illegible] military grade FPGA. Using an innovative patented technique we [illegible] and analyse in the first documented case of its kind, a [illegible] Actel/Microsemi ProASIC3 chips. The backdoor [illegible] itself, it was not present in any firmware [illegible] Emission Analysis (PEA), a technique [illegible] extract the secret key to activate the [illegible] all the security on the chip, [illegible] silicon features, access [illegible] damage the device. [illegible] theft, fraud, [illegible] allows the [illegible] to patch the [illegible] of chips have to [illegible] be physically replaced [illegible]

Undocumented Features!

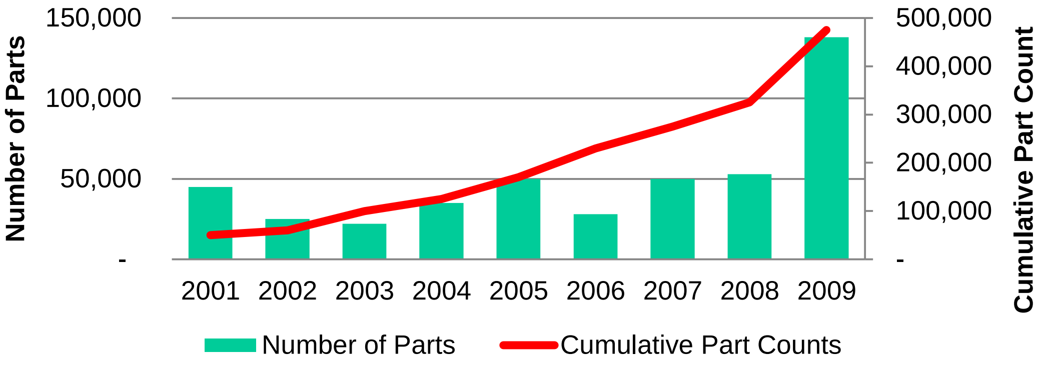
Keywords: Hardware Assu[illegible] hardware Trojans and backdoors

1 Introduction

With the globalisation of semiconductor manufacturing, inte[illegible] vulnerable to malevolent activities in the form of Trojan and backd[illegible] An adversary can introduce Trojans into the design during a stage of [illegible] by modifying the mask at a foundry or fab. It can also be present inside third p[illegible]es' modules or blocks used in the design. Backdoors could be implemented by malicious insiders at the design house. In this paper we demonstrate how a deliberately inserted backdoor and additional functionalities can be found in a highly secure FPGA (field-programmable gate array) chip used in both military and sensitive industrial applications. Trojans can be found using a similar approach, altering the way the scanning is performed slightly. To our knowledge, this is the first documented case of finding a deliberately inserted backdoor in a real world chip.

Several Trojan detection approaches have been proposed in recent years. These can be divided into three major categories. One is full reverse engineering of the chip

Diminishing Manufacturing Sources and Material Shortages (DMSMS) Part Number Counts



Ensuring Confidence in Defense Systems

- ***Threat***: Nation-state, terrorist, criminal, or rogue developer who:
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Traditional Consequences***: Loss of critical data and technology
- ***Emerging Consequences***: Exploitation of manufacturing and supply chain
- Either can result in corruption; loss of confidence in critical warfighting capability

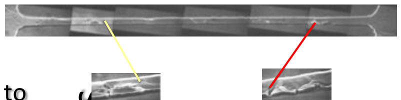
Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

Electronic Reliability Timeline

1950's

Robert Lusser states 60% of failures are due to electronic parts in Army missile



1960's

Failure of aluminum electrolytic capacitors start to appear in military systems.

1970's

E.M. Pohilofsky finds that gold and aluminum are leading cause of field failures in 60's and 70's

1990's

AFRL stood up and the Reliability Assessment Center (Rome Lab) was stood down

1990's

The Army launches the Electronic Equipment Physics-of-Failure Project

2000's

Dielectric failures are proving to be the leading cause for transistor failures in smaller node sizes

1950's — 2000's

1960's

The Minuteman System cost is $30,000,000 for parts improvement by improving processing methods and for reliability testing . RDT&E annual budget is only $16,000,000 for electronic components.

1960's

J.R. Black publishes first paper on electromigration

1970's

First evidence of hot electrons

1980's

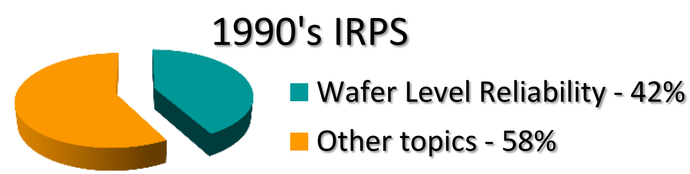
Space shuttle flight is aborted due to IC reliability failure

1997

DMEA stands up

2010

AFRL and NRO stood up HiREV . DMEA added as member later that year.



Note: Other topics include packaging, design for reliability and process

G.H. Ebel, "Reliability Physics in electronics: A Historical View", IEEE Transactions on Reliability, Vol. 47, NO. 3-SP 1998, pp379-389

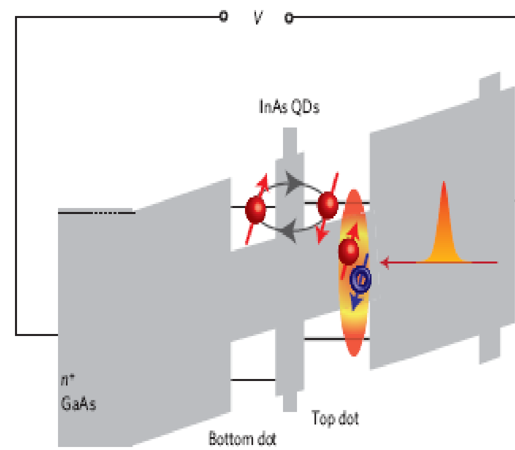
Future Technology Directions

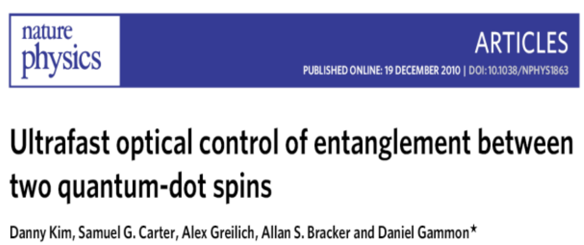
- **New Architectures/Algorithms Toward Cognition**
  - Digital Clock Rates Exceeding 15 GHz
  - Integration of Integrated Photonic Circuits & Electronic IC's Form Extraordinary Powerful Energy Efficient Processors
  - Biomimetic inspired electronics
- **Silicon and other emerging new materials**
  - III-V's Integrated with Si Nano-Wire CMOS; Carbon Based
  - Toward Reduced Power Dissipation
- **Quantum**
  - Information Processing
  - Computing
  - Sensing
  - Key Distribution
- **Unpredictable Technology Revolution Through Scientific Advances**


nature photonics ARTICLES
PUBLISHED ONLINE: XX XX 2013 | DOI: 10.1038/NPHOTON.2013.41

Quantum control of a spin qubit coupled to a photonic crystal cavity

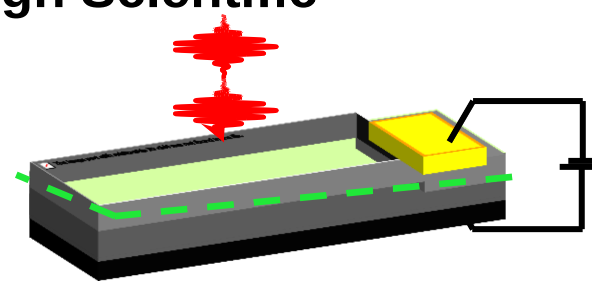
Samuel G. Carter[1†], Timothy M. Sweeney[2†], Mijin Kim[3], Chul Soo Kim[1], Dmitry Solenov[2], Sophia E. Economou[1], Thomas L. Reinecke[1], Lily Yang[2], Allan S. Bracker[1] and Daniel Gammon[1]*




nature physics ARTICLES
PUBLISHED ONLINE: 19 DECEMBER 2010 | DOI: 10.1038/NPHYS1863

Ultrafast optical control of entanglement between two quantum-dot spins

Danny Kim, Samuel G. Carter, Alex Greilich, Allan S. Bracker and Daniel Gammon*



Summary

- DoD S&T aligned to meet priorities for a 21st Century security environment
- Preservation and delivery of advanced technology remains a high priority
- DoD R&E is committed to a healthy Defense Microelectronics and Industry Base
- Future Technology Directions of Microelectronics have enabled the Department and are at the core of their mission